

ABSTRACT OF THE DISCLOSURE

A wireless device, such as a Bluetooth mobility pin is coupled to a biometric device, such as a thumb scanner, providing for wireless communication with a system to which access is desired. The thumb scanner provides a reliable and secure signal based upon biometric measurements, the signal being provided to the pin, which is then uniquely coded to the accessed system. When a workstation or other device having a compatible antenna receives the signal from the pin, the workstation accesses identification data and allows for login of the user based upon the highly secure biometric measurements, and the wireless connection between the pin and the system. The pin will not send the required code unless the coded user of the pin succeeds in scanning the thumbprint or other biometric measurement basis.